DRMS-D 5200.5
DRMS-DDS
December 17, 1998

WEB/INTERNET POLICY
(Supplementation is prohibited.)

A. REFERENCES

1. DLAR 5200.17, Security Requirements for Automated Information And Telecommunications Systems.

2. DoDD 5200.28, Security Requirements for Automated Information Systems (AISs).

3. DLA Internet Policy, May 1997.

4. DLAR 1406.1, Maintaining Discipline.

B. PURPOSE. This document is intended to further define what is presented in the DLA Internet Policy. This document will also clarify and amplify guidelines for Internet usage. This document establishes policy, provides guidance, and assigns responsibilities for the use of the Internet and World Wide Web, Intranets, and electronic mail by military, local nationals, civilian, and contracted personnel of the Defense Reutilization and Marketing Service (DRMS). It applies to all such personnel who use government-furnished resources to disseminate or obtain information via these media.

C. APPLICABILITY AND SCOPE. This directive applies to all offices/directorates of HQ DRMS and all DRMS field activities. This directive promotes the DLA Internet policy (reference A3.) The procedural steps and the individual responsibilities are in consonance with the security requirements of the DLAR 5200.17 (reference A1) and DoDD 5200.28 (reference A2).

D. DEFINITIONS.

1. Accountability. The property that enables activities on an Automated Information System (AIS) to be traced to individuals who may then be held responsible for their actions.

2. Audit. An independent review and examination of system records and activities to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

3. Communications Security. Measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government concerning national security, and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of communications security material and information.

4. Designated Approving Authority (DAA). The official who makes the final determination as to whether an AIS or Data Processing Information (DPI) has sufficiently reduced its operational security risk to merit accreditation and who issues a dated, written accreditation statement authorizing the AIS to operate in a designated security mode and at a defined level of risk. The DAA must be at an appropriate organizational level with authority to accept the risk residual in an AIS or DPI.

5. Free Activities/sites. These are addresses that may be used that do not charge for services. The government is in no way obligated to pay any costs for usage.

6. Information. Knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium.

7. Internet. "Internet" refers to the global information system that –

(i) is logically linked together by a globally unique address space based on the Internet Protocol (IP)

(ii) or its subsequent extensions/follow-ons; is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and

(iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein."

8. Need-To-Know. The necessity for access to, knowledge of, or possession of specific information required to carry out official duties.

9. Network. A communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include AISs, packet switches, telecommunications controllers, key distribution centers, and technical control devices.

10. Official Duties. Duties addressed in employee’s current Position Description (PD) or additional duties assigned by supervisor.

11. Resource. In an AIS, anything used or consumed while performing a function. The categories of resources are: time, information, objects (information containers), or processors.

12. Security Incidents. Security events which violate neither laws nor regulations (e.g., locking up a terminal by exceeding the allowed number of tries to correctly enter a logon ID or password; unexplained access by a user to an otherwise denied object).

13. Security Violations. Actions of two types: those which violate one or more laws of a duly constituted civil authority and those which violate DLA regulations.

14. Telecommunications. A general term expressing data transmission between computing systems and remotely located devices via a unit that performs the necessary format conversion and controls the rate of transmission.

E. POLICY

1. The Internet may be used for official purposes. Under no circumstance will classified information be placed on or made accessible by the Internet. Official use is further defined as follows:

a. Obtaining or exchanging information to support DLA or DoD missions could include researching manufacturer’s information or accessing information or regulations from another government web site.

b. Obtaining or exchanging information that enhances the professional skills of DLA employees, thereby improving job performance and benefiting the agency – such as improving research, report writing, or communications skills.

c. Improving an employee’s formal education, when approved by an immediate supervisor. Requests must document how this will improve the employee’s formal education and why this is in the best interest to the Federal Government. Requests must be submitted in hardcopy or email to the immediate supervisor. Hardcopy or email requests will be signed by the supervisor and returned to the employee, or returned with a negative response with reasons cited. Supervisors will decide if employees may engage in this activity on company time or personal time on a case by case basis. The request will be documented whether the employee is allowed to perform this activity on government or personal time. This applies to free activities only. If charges are incurred, these activities must be treated as

training and the appropriate documents with fund cites must be submitted. Employees are not allowed to obligate funds.

2. NON-OFFICIAL USE as authorized in the DLA Internet Policy is hereby approved by the DRMS Commander. However, there are limitations. NON-OFFICIAL USE is further defined and restricted as follows:

a. The use must not adversely affect the employee's performance of official duties. Any non-official use must take place on the employee's own time, such as breaks, lunch or before/after duty hours. An employee's job must not suffer as a result of using the Internet. If an employee's supervisor determines job performance is affected, Internet privileges may be limited or revoked entirely. This will be done on a case by case basis, so as not to punish everyone for the few who may abuse this privilege.

b. Internet usage must also serve such legitimate public interests as:

(1) Enhancing employees' professional skills. These skills should have some applicability to the current job, the discipline in which the employee received a college degree, or an area which the government has sponsored substantial training. However, it does not have to deal with an ongoing issue or problem in the current job, as that is permitted as 'official' use. These are skills, not mere knowledge, that are being enhanced. Examples of this might be acquiring a better understanding of statistical measures, reviewing medical or health/wellness information to better deal with clients, taking courses or training oriented toward some professional skills or investigating new problem solving techniques.

(2) Educating the employee on the use of the Internet as a business and communication tool. This could include accessing other government agency's web sites, accessing vendors' web sites to retrieve information, or looking at web presentation techniques from valid and respectable sites. See prohibited use section for examples not allowed.

(3) Improving the morale of employees who are stationed away from home for extended periods.

(4) Enabling employee's participation in professional or civic associations that would not in anyway be detrimental to the U.S. Government. Examples would include charitable organizations, chamber of commerce, business groups, management associations, computer associations or groups, or civic events.

(5) Helping military and civilian personnel to seek job opportunities in the federal government.

3. Prohibited use covers illegal, immoral, or improper acts such as gambling, visiting pornography sites, soliciting for personal gain, personal transactions other than previously approved (i.e. Thrift Savings site), storing personal information, playing games, use of non-governmental CDs for personal entertainment or engaging in chain letters. Breaches of security, such as sharing passwords for protected web sites, are also prohibited. The items listed in this section are not allowed at any time. The following information is provided to DRMS employees for clarification:

a. Downloading copyrighted software without express permission. Permission must be received from the originator of the software, and any time constraints must be obeyed (i.e., 30 day demo). Demo software must be removed at the end of the demo time period. Written permission must also be received from the employee's immediate supervisor. Software must also be approved by the PDB (Project Development Board) and registered with DRMS-C EUC.

b. Downloading without ensuring protection against viruses. Virus protection software is installed on all LAN and personal computers. Intentionally removing or bypassing the software is prohibited.

c. Misrepresenting personal opinion as official information. Employees cannot send out email or messages to newsgroups or interact with web sites espousing personal opinion as official government policy or pronouncement. The use does not put Federal Government resources to uses that would reflect adversely on DOD or the DOD Component (such as involving commercial activities; unofficial advertising, soliciting or selling, violation of statute or regulation; and other uses that are incompatible with public service).

d. Approval - The Public Affairs Office and the Designated Approving Authority must be aware and approve of all information contained on DRMS's web site. Day to day business does not have to be cleared (i.e. daily solicitations/bits). This requirement includes not only DRMS's home page, but also all applications interfacing or using the World Wide Web as part of their processing infrastructure.

e. Conventions and Etiquette - E-mail. No profanity, threats, intent to commit or commission of illegal or improper acts are allowed. The Federal Government reserves the right to monitor all email sent, received, or stored if improper use of government ADP resources is suspected.

f. File Transfers. File transfers are a legitimate way of retrieving data from a remote source. The same Internet rules apply. The data being transferred must be applicable under official or non-official use.

g. Chat. Accessing chat rooms for the purpose of soliciting assistance on job related problems is authorized. However, the chat room must be oriented to solving such problems. Accessing chat rooms for any other purpose is not authorized. Chat rooms must be used as a communication tool.

h. Security.

(1) There is very little security on the Internet. However, auditing is available. The Command Security Office staff reserves the right to review and monitor all audit trails. All other attempts within the agency to review audit trails must be coordinated through the Command Security office. Any infractions found will be turned over to the appropriate areas for action. See DLAR 1406.1, Maintaining Discipline.

(2) Certain areas of the DRMS web pages are restricted to only users with .mil or .gov IP addresses or who have been authorized access to those pages. Access to internal pages are approved only by the appointed approving authority. If required, additional lockdowns will be strictly enforced.

4. DRMS HQ is responsible for the establishment of all WEB Servers for DRMS. Under no circumstances shall DRMO personnel create pages or establish web servers with commercial or government entities for DRMS information without prior written consent from DRMS Web Administration and Public Affairs.

F. RESPONSIBILITIES

1. Manager will:

a. Approve or disapprove web usage or web page development within the office. It is assumed that approval has been granted for web usage unless previously rescinded.

b. Give approval in writing for any special time consuming web accesses.

c. Ensure that users know the rules and regulations dealing with web usage.

d. Ensure that employees are informed upon implementation of this policy and, at a minimum, annually thereafter of their responsibilities regarding use of the WEB/Internet.

2. DRMS users will:

a. Ensure that anti-virus detection is running on system.

b. Have supervisor's approval for web accessing.

c. Have supervisor's approval in writing for special web accesses such as downloading software, doing classes or other duty time consuming web tasks.

d. Adhere to the guidelines and procedures explained in this document.

3. Information System Security Officer (ISSO) will:

a. Ensure that users know the operating procedures in accordance with regulations.

b. Implement security procedures for the activity's web security program.

c. Maintain this directive in a current status and review it annually.

4. End User Computing (EUC) will:

a. Ensure that the most current version of the approved anti-virus program has been installed.
b. Ensure that a current version of the anti-virus program is available for downloading from the web.

5. Web masters will:

a. Identify the access requirements for DRMS web page.
b. Provide guidance on web usage.

G. EFFECTIVE DATE AND IMPLEMENTATION. This directive is effective upon its publication.

H. INFORMATION REQUIREMENTS. Reserved for future use.

BY ORDER OF THE COMMANDER

ROLAND V. JOHNSON
Lieutenant Colonel, OD, ARNG
Executive Officer